PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-140450
(43)Date of publication of application : 17.05.2002

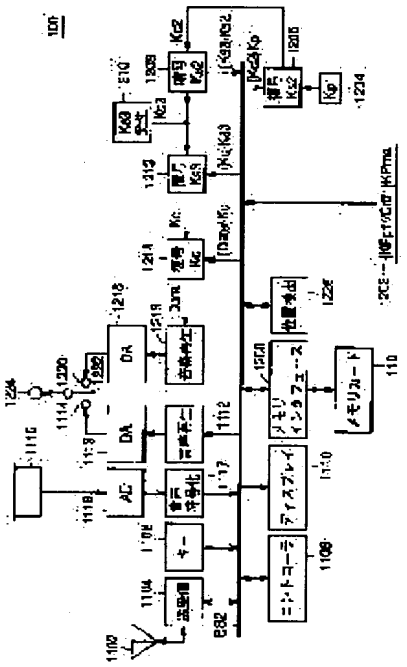
(51)Int.Cl. G06F 17/60
G10K 15/02
G10L 19/00
H04M 1/00
H04M 11/00
// G06F 13/00

(21)Application number : 2000-334201
(22)Date of filing : 01.11.2000

(71)Applicant : SANYO ELECTRIC CO LTD
(72)Inventor : MATSUURA TAKENORI

(54) DATA DISTRIBUTING SYSTEM AND DATA TERMINAL EQUIPMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data distributing system and data terminal equipment capable of receiving enciphered contents data related with positional information.
SOLUTION: A portable telephone set 100 is provided with a position detecting part 1226. The position detecting part 1226 detects the present position of the portable telephone set 100 by a GPS. A controller 1106 transmits the present position of the portable telephone set 100 detected by the position detecting part 1226 through a transmitting/receiving part 1104 to a distributing server at the time requesting the distribution of the enciphered contents data. Then, the controller 1106 receives the enciphered contents data related with the present position through the transmitting/receiving part 1104, and records and/or reproduces the enciphered contents data to/from a memory card 110.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

What is claimed is:

1. A data terminal device for receiving an enciphered content data that is content data enciphered, and a license for reproducing the enciphered content data from a distributing server, and for recording and/or reproducing the enciphered content data and the license to/from a data recording device, the data terminal device comprising:

a transmitting/receiving part for performing a communication with the external;

an interface for controlling data transfer with the data recording device;

a key operating part for inputting a direction; and

a control part,

wherein the control part receives an enciphered content data related with a present position and a license for reproducing the enciphered content data from the distributing server via the transmitting/receiving part, in response to a request for receiving the enciphered content data input through the key operating part, and records the received enciphered content data and the license in the data recording device via the interface.

2. The data terminal device of claim 1, wherein the control part transmits the present position as position information as well as a distribution request of the enciphered content data to the distributing server via the transmitting/receiving part.

3. The data terminal device of claim 2, further comprising a position detecting part for detecting the present position, wherein the control part transmits the detected present position to the distributing server via the transmitting/receiving part.

4. The data terminal device of claim 3, wherein the position detecting part detects the present position by a global positioning system.

参考技術

㈱エムテック関東 (5)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－140450
（Ｐ2002－140450Ａ）
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
G06F 17/60	142	G06F 17/60	142	5K027
	302		302 E	5K101
	332		332	
	502		502	
	506		506	

審査請求　未請求　請求項の数16　ＯＬ　（全25頁）　最終頁に続く

(21)出願番号　特願2000－334201（Ｐ2000－334201）

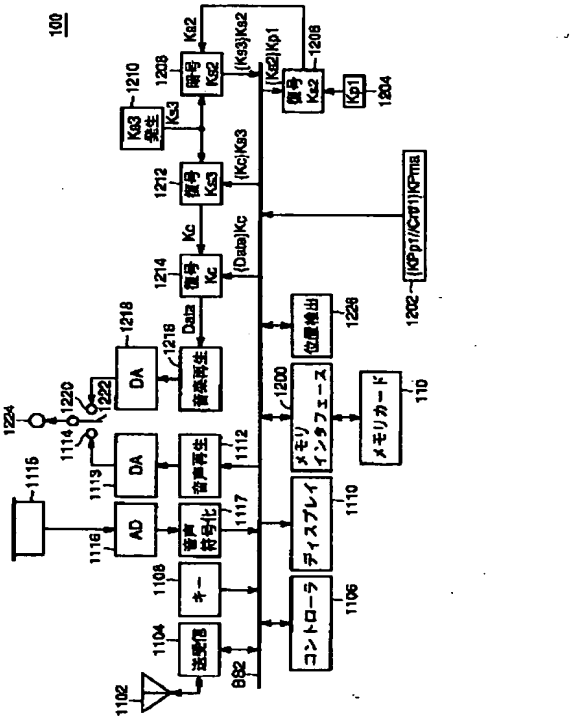
(22)出願日　平成12年11月１日(2000.11.1)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　松浦　竹典
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

Ｆターム(参考)　5K027 AA11 CC08 EE11 HH00 HH24
5K101 KK18 LL11 NN15 PP04 UU19

(54)【発明の名称】データ配信システムおよびデータ端末装置

(57)【要約】
【課題】　位置情報に関連する暗号化コンテンツデータを受信可能なデータ配信システムおよびデータ端末装置を提供する。
【解決手段】　携帯電話機１００は、位置検出部１２２６を備える。位置検出部１２２６は、ＧＰＳによって携帯電話機１００の現在位置を検出する。コントローラ１１０６は、暗号化コンテンツデータの配信要求を行なうとき、位置検出部１２２６が検出した携帯電話機１００の現在位置を送受信１１０４を介して配信サーバへ送信する。そして、コントローラ１１０６は、現在位置に関連する暗号化コンテンツデータを送受信部１１０４を介して受信し、メモリカード１１０に記録および／または再生する。



1

【特許請求の範囲】

【請求項１】　コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを再生するためのライセンスとを配信サーバから受信し、前記暗号化コンテンツデータおよび前記ライセンスをデータ記録装置に記録および／または再生するデータ端末装置であって、
外部との通信を行なう送受信部と、
前記データ記録装置とのデータ授受を制御するインタフェースと、
指示を入力するためのキー操作部と、
制御部とを備え、
前記制御部は、前記キー操作部を介して入力された暗号化コンテンツデータの受信要求に応じて、現在位置に関連する暗号化コンテンツデータと前記暗号化コンテンツデータを再生するライセンスとを前記送受信部を介して前記配信サーバから受信し、その受信した暗号化コンテンツデータとライセンスとを前記インタフェースを介して前記データ記録装置に記録する、データ端末装置。

【請求項２】　前記制御部は、前記暗号化コンテンツデータの配信要求とともに前記現在位置を位置情報として前記送受信部を介して前記配信サーバへ送信する、請求項１に記載のデータ端末装置。

【請求項３】　前記現在位置を検出する位置検出部をさらに備え、
前記制御部は、前記検出した現在位置を前記送受信部を介して前記配信サーバへ送信する、請求項２に記載のデータ端末装置。

【請求項４】　前記位置検出部は、グローバルポジショニングシステムによって前記現在位置を検出する、請求項３に記載のデータ端末装置。

【請求項５】　前記制御部は、コンサート会場の位置を前記現在位置として前記送受信部を介して前記配信サーバへ送信し、前記コンサート会場で演奏されている曲と同じ暗号化音楽データを前記送受信部を介して受信する、請求項１から請求項４のいずれか１項に記載のデータ端末装置。

【請求項６】　前記制御部は、前記暗号化音楽データを再生するライセンスを通常料金よりも安い料金で受信する、請求項５に記載のデータ端末装置。

【請求項７】　表示部をさらに備え、
前記制御部は、前記現在位置に関連する画像データを前記送受信部を介して受信し、その受信した画像データを前記表示部に表示する、請求項５または請求項６に記載のデータ端末装置。

【請求項８】　前記暗号化コンテンツデータは暗号化音楽データであり、
前記暗号化音楽データを再生した音楽データを外部装置へ出力するための端子をさらに含み、
前記制御部は、前記配信サーバにおいて再生された音楽データを受信し、その受信した音楽データを前記端子へ与え、前記音楽データの受信要求が前記キー操作部から入力されると前記配信サーバへ暗号化音楽データの配信要求を送信する、請求項１に記載のデータ端末装置。

2

【請求項９】　コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを再生するライセンスとを保持する配信サーバと、
前記配信サーバから前記暗号化コンテンツデータおよび前記ライセンスを受信し、その受信した暗号化コンテンツデータおよびライセンスをデータ記録装置に記録および／または再生するデータ端末装置とを備え、
前記配信サーバは、前記暗号化コンテンツデータの配信要求を送信した前記データ端末装置の現在位置に関連した暗号化コンテンツデータを前記データ端末装置へ配信する、データ配信システム。

【請求項１０】　前記配信サーバは、前記現在位置に関連した暗号化コンテンツデータの配信要求を受信すると、電話網によって位置情報を取得する位置情報センターから前記現在位置を受信する、請求項９に記載のデータ配信システム。

【請求項１１】　前記配信サーバは、前記データ端末装置から前記現在位置を取得する、請求項９に記載のデータ配信システム。

【請求項１２】　前記配信サーバは、携帯電話網を構成する基地局から前記現在位置を取得する、請求項９に記載のデータ配信システム。

【請求項１３】　前記配信サーバは、前記現在位置を受信してからその現在位置に関連する暗号化コンテンツデータを検索し、その検索した暗号化コンテンツデータを前記データ端末装置へ配信する、請求項９から請求項１２のいずれか１項に記載のデータ配信システム。

【請求項１４】　前記配信サーバは、予め位置情報によって分類された暗号化コンテンツデータを保持し、前記現在位置を受信するとその現在位置に関連する暗号化コンテンツデータを前記データ端末装置へ配信する、請求項９から請求項１２のいずれか１項に記載のデータ配信システム。

【請求項１５】　前記配信サーバは、コンサート会場の位置を前記現在位置として前記データ端末装置から受信し、前記コンサート会場で演奏されている曲と同じ暗号化音楽データを前記データ端末装置へ配信する、請求項９から請求項１４のいずれか１項に記載のデータ配信システム。

【請求項１６】　前記配信サーバは、前記暗号化音楽データを再生するライセンスを通常料金よりも安い料金で前記データ端末装置へ配信する、請求項１５に記載のデータ配信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コピーされた情

報に対する著作権保護を可能とするデータ配信システムおよびデータ端末装置に関するものである。

【０００２】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】

【発明が解決しようとする課題】しかし、暗号化コンテンツデータの配信をサーバへ要求する場合、ユーザとしては、現在位置に関連する暗号化コンテンツデータの配信を要求したい場合がある。特に、旅行などで各地域を訪れた場合、その地域に関連する音楽を聴きたいときがあり、その場合、その地域に関連する音楽を迅速に受信できれば便利である。

【００１５】それゆえに、この発明の目的は、位置情報に関連する暗号化コンテンツデータを受信可能なデータ配信システムおよびデータ端末装置を提供することである。

【００１６】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを再生するためのライセンスとを配信サーバから受信し、暗号化コンテンツデータおよびライセンスをデータ記録装置に記録および／または再生するデータ端末装置

であって、外部との通信を行なう送受信部と、データ記録装置とのデータ授受を制御するインタフェースと、指示を入力するためのキー操作部と、制御部とを備え、制御部は、キー操作部を介して入力された暗号化コンテンツデータの受信要求に応じて、現在位置に関連する暗号化コンテンツデータと暗号化コンテンツデータを再生するライセンスとを送受信部を介して配信サーバから受信し、その受信した暗号化コンテンツデータとライセンスとをインタフェースを介してデータ記録装置に記録する。

【００１７】この発明によるデータ端末装置は、データ端末装置の現在位置に関連する暗号化コンテンツデータと、その暗号化コンテンツデータを再生するライセンスとを受信し、データ記録装置に記録および／または再生を行なう。

【００１８】したがって、この発明によれば、移動中などに各地域に関連する音楽を楽しむことができる。

【００１９】好ましくは、データ端末装置の制御部は、暗号化コンテンツデータの配信要求とともに現在位置を位置情報として送受信部を介して配信サーバへ送信する。

【００２０】データ端末装置においては、制御部は、暗号化コンテンツデータの配信要求を配信サーバへ送信するとともに、データ端末装置の現在位置を配信サーバへ送信する。つまり、データ端末装置は、位置情報の発信機能を有する。そうすると、配信サーバは、受信した現在位置に関連する暗号化コンテンツデータを抽出し、データ端末装置へ配信する。

【００２１】したがって、この発明によれば、正確な現在位置を配信サーバへ送信することができる。

【００２２】好ましくは、データ端末装置は、現在位置を検出する位置検出部をさらに備え、制御部は、検出した現在位置を送受信部を介して配信サーバへ送信する。

【００２３】位置検出部は、データ端末装置の現在位置を検出し、制御部は位置検出部が検出した現在位置を受取り、送受信部を介して配信サーバへ送信する。つまり、データ端末装置は、位置情報の検出および発信機能を有する。

【００２４】したがって、この発明によれば、データ端末装置は自ら位置検出と、その検出した位置情報を配信サーバへ送信することができる。

【００２５】好ましくは、データ端末装置の位置検出部は、グローバルポジショニングシステムによって現在位置を検出する。

【００２６】位置検出部は、少なくとも３個または４個の衛星から送られてくる信号に基づいてデータ端末装置の現在位置を検出する。そして、制御部は位置検出部がグローバルポジショニングシステム（ＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ））によって検出した現在位置を受取り、配信サーバへ送信する。

【００２７】したがって、この発明によれば、データ端末装置の現在位置を正確に検出することができる。その結果、データ端末装置は、データ端末装置の存在する地名に関連する暗号化コンテンツデータを正確に受信できる。

【００２８】好ましくは、データ端末装置の制御部は、コンサート会場の位置を現在位置として送受信部を介して配信サーバへ送信し、コンサート会場で演奏されている曲と同じ暗号化音楽データを送受信部を介して受信する。

【００２９】データ端末装置の制御部は、コンサート会場の位置を位置情報として配信サーバへ送信する。配信サーバは、位置情報に基づいてコンサート会場を抽出し、そのコンサート会場で演奏されている音楽データをデータ端末装置へ配信する。

【００３０】したがって、この発明によれば、コンサート会場へ入れなくてもコンサート会場で演奏される音楽を聴くことができる。

【００３１】好ましくは、データ端末装置の制御部は、コンサート会場の位置を配信サーバへ送信するとき、暗号化音楽データを再生するライセンスを通常料金よりも安い料金で受信する。

【００３２】データ端末装置の制御部は、コンサート会場の位置を配信サーバへ送信し、配信サーバはコンサート会場で演奏されている暗号化音楽データと、その暗号化音楽データを再生するライセンスとをデータ端末装置へ送信するとき、通常の料金よりも安い料金をライセンスの配信に対して課金する。

【００３３】したがって、ユーザは通用よりも安い料金で音楽データを受信して聴くことができる。

【００３４】好ましくは、データ端末装置は、表示部をさらに備え、制御部は、現在位置に関連する画像データを送受信部を介して受信し、その受信した画像データを表示部に表示する。

【００３５】データ端末装置の制御部は、データ端末装置の現在位置に関連する暗号化コンテンツデータとともに現在位置に関連する画像データを受信し、その受信した画像データを表示部に表示する。

【００３６】したがって、この発明によれば、現在位置に関連する音楽データをその地方の景色を見ながら聴くことができる。

【００３７】好ましくは、暗号化コンテンツデータは暗号化音楽データであり、データ端末装置は、暗号化音楽データを再生した音楽データを外部装置へ出力するための端子をさらに含み、制御部は、配信サーバにおいて再生された音楽データを受信し、その受信した音楽データを端子へ与え、音楽データの受信要求がキー操作部から入力されると配信サーバへ暗号化音楽データの配信要求を送信する。

【００３８】データ端末装置の制御部は、配信サーバにおいて再生された音楽データを受信し、その受信した音楽データを外部装置へ出力するための端子に与える。そして、制御部は、外部装置へ出力した音楽データの受信要求がキー操作部から入力されると、配信サーバへ暗号化音楽データの配信要求を行なう。つまり、音楽データの試聴がなされ、最終的に音楽データの受信要求がデータ端末装置に入力されてから配信サーバへ暗号化コンテンツデータの配信要求がなされる。

【００３９】したがって、この発明によれば、ユーザは本当に聴きたい音楽データだけを受信して聴くことができる。

【００４０】この発明によるデータ配信システムは、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを再生するライセンスとを保持する配信サーバと、配信サーバから暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータおよびライセンスをデータ記録装置に記録および／または再生するデータ端末装置とを備え、配信サーバは、暗号化コンテンツデータの配信要求を送信したデータ端末装置の現在位置に関連した暗号化コンテンツデータをデータ端末装置へ配信する。

【００４１】この発明によるデータ配信システムにおいては、データ端末措置は暗号化コンテンツデータの配信要求を配信サーバへ行ない、配信サーバはデータ端末装置の現在位置に関連した暗号化コンテンツデータをデータ端末装置へ配信する。

【００４２】したがって、この発明によれば、データ端末装置のユーザは、現在位置に関連する暗号化コンテンツデータを配信サーバから受信してコンテンツを再生することができる。

【００４３】好ましくは、配信サーバは、現在位置に関連した暗号化コンテンツデータの配信要求を受信すると、電話網によって位置情報を取得する位置情報センターから現在位置を受信する。

【００４４】配信サーバは、データ端末装置から暗号化コンテンツデータの配信要求を受信すると、位置情報センターからデータ端末装置の現在位置を受信する。そして、配信サーバは、受信した現在位置に関連する暗号化コンテンツデータをデータ端末装置へ配信する。つまり、配信サーバは、データ端末装置が配信サーバへ暗号化コンテンツデータの配信要求を行なう経路と異なる経路からデータ端末装置の現在位置を取得する。

【００４５】したがって、この発明によれば、データ端末装置が現在位置を検出する機能を備えていなくても、現在位置に関連した暗号化コンテンツデータを受信できる。

【００４６】好ましくは、配信サーバは、データ端末装置からデータ現在位置を取得する。配信サーバは、暗号化コンテンツデータの配信要求とデータ端末装置の現在位置とをデータ端末装置から受信する。

【００４７】したがって、この発明によれば、データ端末装置の現在位置を正確に検知できる。

【００４８】好ましくは、配信サーバは、携帯電話網を構成する基地局からデータ端末装置の現在位置を取得する。

【００４９】配信サーバは、携帯電話網を構成する基地局からデータ端末装置の現在位置を取得する。

【００５０】したがって、この発明によれば、データ端末装置が携帯電話網を介して配信サーバへアクセスすることにより、データ端末装置は現在位置を配信サーバへ送信しなくても、現在位置に関連する暗号化コンテンツデータを受信できる。

【００５１】好ましくは、配信サーバは、現在位置を受信してからその現在位置に関連する暗号化コンテンツデータを検索し、その検索した暗号化コンテンツデータをデータ端末装置へ配信する。

【００５２】配信サーバは、データ端末装置の現在位置を受信すると、現在位置に関連する暗号化コンテンツデータを検索し、データ端末装置へ配信する。

【００５３】したがって、この発明によれば、配信サーバへ送信されるデータ端末装置の現在位置に応じた暗号化コンテンツデータをデータ端末装置へ配信できる。

【００５４】好ましくは、配信サーバは、予め位置情報によって分類された暗号化コンテンツデータを保持し、現在位置を受信するとその現在位置に関連する暗号化コンテンツデータをデータ端末装置へ配信する。

【００５５】配信サーバは、データ端末装置の現在位置を受信すると、その受信した現在位置に関連する暗号化コンテンツデータを予め分類した暗号化コンテンツデータから選択し、データ端末装置へ配信する。

【００５６】したがって、この発明によれば、現在位置に関連する暗号化コンテンツデータを迅速にデータ端末装置へ配信できる。

【００５７】好ましくは、配信サーバは、コンサート会場の位置を現在位置としてデータ端末装置から受信し、コンサート会場で演奏されている曲と同じ暗号化音楽データをデータ端末装置へ配信する。

【００５８】配信サーバは、コンサート会場の位置を現在位置としてデータ端末装置から受信し、そのコンサート会場で演奏されている暗号化音楽データをデータ端末装置へ配信する。

【００５９】したがって、この発明によれば、コンサート会場へ入れなくてもコンサート会場で演奏されている音楽を聴くことができる。

【００６０】好ましくは、配信サーバは、暗号化音楽データを再生するライセンスを通常料金よりも安い料金でデータ端末装置へ配信する。

【００６１】配信サーバは、データ端末装置の現在位置としてコンサート会場の位置を受信したとき、そのコン

サート会場で演奏されている暗号化音楽データを通常よりも安い料金でデータ端末装置で配信する。

【００６２】したがって、ユーザは、通常よりも安い料金でコンサート会場で演奏されている音楽を聴くことができる。

【００６３】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００６４】図１は、本発明による携帯端末装置が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００６５】なお、以下では携帯電話網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【００６６】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバに中継する。著作権の存在する音楽データを管理するライセンスサーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【００６７】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００を介して暗号化コンテンツデータとライセンスとを配信する。

【００６８】図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

【００６９】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００７０】以下では、このようなライセンスサーバ１０と配信キャリア２０とを併せて、配信サーバ３０と総称することにする。

【００７１】また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【００７２】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ３０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００７３】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００７４】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、また、第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【００７５】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機とも言う。以下同じ））に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００７６】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００７７】まず、配信サーバ３０より配信されるデータについて説明する。Ｄａｔａは、音楽データ等のコンテンツデータである。コンテンツデータＤａｔａには、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがこの形式で配信サーバ３０より携帯電話ユーザに配布される。

【００７８】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００７９】さらに、配信サーバ３０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著

作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄａｔａ－ｉｎｆが配布される。また、配信サーバ３０からの暗号化コンテンツデータおよびライセンス鍵等の配信を特定するための管理コードであるトランザクションＩＤが配信サーバ３０と携帯電話機１００との間でやり取りされる。さらに、ライセンス情報としては、コンテンツデータＤａｔａを識別するためのコードであるコンテンツＩＤおよびライセンスの発行を特定できる管理コードであるライセンスＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード）のアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１およびデータ再生端末における制御情報である再生期限ＡＣ２等が存在する。以後、ライセンス鍵ＫｃとコンテンツＩＤとライセンスＩＤと再生回数期限ＡＣ１と再生期限ＡＣ２とを併せて、ライセンスと総称することとする。

【００８０】図３は、図１に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【００８１】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【００８２】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機およびメモリカードのクラスをリストアップした禁止クラスリストデータＣＲＬが含まれる。

【００８３】禁止クラスリストデータＣＲＬは、配信サーバ３０内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス鍵等のライセンスを配信する際の日時を基準として、携帯電話機から受取った禁止クラスリストの更新の有無を判断し、更新されていないとき、更新された禁止クラスリストを携帯電話機に配信する。また、禁止クラスリストの変更については、変更点のみを反映した差分データＣＲＬ＿ｄａｔを配信サーバ３０側より発生して、これに応じてメモリカード内の禁止クラスリストＣＲＬが書替えられる構成とするも可能である。また、禁止クラスリストのバージョンについては、ＣＲＬ＿ｖｅｒをメモリカード側より出力し、これを配信サーバ３０側で確認することによってバージョン管理を実行する。差分データＣＲＬ＿ｄａｔには新たなバージョンの情報も含まれる。

【００８４】このように、禁止クラスリストＣＲＬを、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードへのライセンス鍵の供給を禁止する。このため、携帯電話機ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【００８５】このように、メモリカード内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【００８６】携帯電話機およびメモリカードには固有の公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉがそれぞれ設けられ、公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉは携帯電話機に固有の秘密復号鍵Ｋｐｎおよびメモリカード固有の秘密復号鍵Ｋｍｃｉによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【００８７】また、データ再生端末（携帯電話機）およびメモリカードのクラス証明書として、ＣｒｔｆｎおよびＣｍｃｉがそれぞれ設けられる。これらのクラス証明書は、メモリカードおよびコンテンツ再生端末のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【００８８】これらのメモリカードおよびコンテンツ再生端末固有の公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａおよび｛ＫＰｐｎ／／Ｃｒｔｆｎ｝ＫＰｍａの形式で、出荷時にメモリカードおよびデータ再生端末（携帯電話機）にそれぞれ記録される。後ほど詳細に説明するが、ＫＰｍａは配信システム全体で共通の公開認証鍵である。

【００８９】図４は、図１に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【００９０】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ３０、携帯電話機１００、およびメモリカード１

１０において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００９１】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００９２】これらのセッションキーＫｓ１～Ｋｓ３は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００９３】また、メモリカード１１０内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍと、公開暗号鍵ＫＰｍで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Ｋｍが存在する。

【００９４】図５は、図１に示したライセンスサーバ１０の構成を示す概略ブロック図である。

【００９５】ライセンスサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための情報データベース３０４と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベースに保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、コンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、ＣＲＬデータベース３０６、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００９６】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａを復号するための公開認証鍵を保持する認証鍵保持部３１３と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰｍａによって復号処理を行なう復号処理部３１２と、セッションキー発生部３１６により生成されたセッションキーＫｓ１を復号処理部３１２によって得られた公開暗号鍵ＫＰｍｃｉを用いて暗号化して、バスＢＳ１に出力するための暗号処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００９７】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよび再生期限ＡＣ２を、復号処理部３２０によって得られたメモリカード固有の公開暗号鍵ＫＰｍによって暗号化するための暗号処理部３２６と、暗号処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号処理部３２８とを含む。

【００９８】ライセンスサーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００９９】図６は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【０１００】携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのバスＢＳ２と、バスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６とを含む。

【０１０１】携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与えるためのキー操作部１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、バスＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２とを含む。

【０１０２】携帯電話機１００は、さらに、音声再生部１１１２の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１１１３と、ＤＡ変換器１１１３の出力を外部出力装置等へ出力するための端子１１１４とを含む。

【０１０３】携帯電話機１００は、さらに、通常の通話動作において、携帯電話機１００のユーザが話した音声信号を入力するマイク１１１５と、マイク１１１５からの音声信号をアナログ信号からディジタル信号に変換するＡＤ変換器１１１６と、ＡＤ変換器１１１６からのディジタル信号を所定の方式に従って符号化してバスＢＳ２へ与える音声符号化部１１１７とを含む。

【０１０４】携帯電話機１００は、さらに、配信サーバ３０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理を行なうための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００とを含む。

【０１０５】携帯電話機１００は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｒｔｆ１を公開復号鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを保持する認証データ保持部１２０２を含む。ここで、携帯電話機（データ端末装置）１００のクラスｎは、ｎ＝１であるとする。

【０１０６】携帯電話機１００は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１２０４と、バスＢＳ２から受けたデータをＫｐ１によって復号しメモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１２０６とを含む。

【０１０７】携帯電話機１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１２１０と、発生されたセッションキーＫｓ３を復号処理部１２０６によって得られたセッションキーＫｓ２によって暗号化しバスＢＳ２に出力する暗号処理部１２０８とを含む。

【０１０８】携帯電話機１００は、さらに、バスＢＳ２上のデータをセッションキーＫｓ３によって復号して出力する復号処理部１２１２と、バスＢＳ２より暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受けて、復号処理部１２１２より取得したライセンス鍵Ｋｃによって復号しコンテンツデータを出力する復号処理部１２１４と、復号処理部１２１４の出力を受けてコンテンツデータを再生するための音楽再生部１２１６と、音楽再生部１２１６の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１２１８とを含む。

【０１０９】携帯電話機１００は、さらに、ＤＡ変換器１１１３とＤＡ変換器１２１８との出力を受けて、動作モードに応じて選択的に端子１１１４または端子１２２０から出力するためのスイッチ１２２２と、スイッチ１２２２の出力を受けて、ヘッドホーン１３０と接続するための接続端子１２２４と、携帯電話機１００の現在位置を検出する位置検出部１２２６とを含む。

【０１１０】ここで、位置検出部１２２６は、ＧＰＳによって携帯電話機１００の現在位置を検出する。ＧＰＳを用いることによって、携帯電話機１００は、約１００ｍの精度で現在位置を特定することができる。

【０１１１】また、位置検出部１２２６は、相対測位方式（ディファレンシャルＧＰＳ（Ｄｉｆｅｒｅｎｔｉａｌ　ＧＰＳ））によって携帯電話機１００の現在位置を検出してもよい。この、相対測位方式とは、基準点の位置とＧＰＳによって検出した携帯電話機１００の位置とを照合比較して衛星系、伝搬系等による誤差を除去して精度の高い位置を検出する方式である。

【０１１２】なお、図６においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【０１１３】携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１１４】図７は、メモリカード１１０の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｃｉおよびＫｍｃｉが設けられ、メモリカードのクラス証明書Ｃｍｃｉが設けられるが、メモリカード１１０においては、これらは自然数ｉ＝１でそれぞれ表わされるものとする。

【０１１５】したがって、メモリカード１１０は、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａを保持する認証データ保持部１４００と、メモリカードの種類ごとに設定される固有の復号鍵であるＫｍｃ１を保持するＫｍｃ１保持部１４０２と、メモリカードごとに固有に設定される秘密復号鍵Ｋｍ１を保持するＫｍ１保持部１４２１と、Ｋｍ１によって復号可能な公開暗号鍵ＫＰｍ１を保持するＫＰｍ１保持部１４１６とを含む。認証データ保持部１４００は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵ＫＰｍｃlおよびクラス証明書Ｃｍｃ１を公開認証鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａとして保持する。

【０１１６】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【０１１７】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１２０１を介

して授受するインタフェース１４２３と、インタフェース１４２３との間で信号をやり取りするバスＢＳ３と、バスＢＳ３にインタフェース１４２３から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Ｋｍｃ１をＫｍｃ１保持部１４０２から受けて、配信サーバ３０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４０４と、ＫＰｍａ保持部１４１４から認証鍵ＫＰｍａを受けて、バスＢＳ３に与えられるデータからＫＰｍａによる復号処理を実行して復号結果を暗号処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してバスＢＳ３に出力する暗号処理部１４０６とを含む。

【０１１８】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られる公開暗号鍵ＫＰｐｎもしくはＫＰｍｃｉによって暗号化してバスＢＳ３に送出する暗号処理部１４１０と、バスＢＳ３よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号し、復号結果をバスＢＳ４に送出する復号処理部１４１２とを含む。

【０１１９】メモリカード１１０は、さらに、バスＢＳ３上のデータを公開暗号鍵ＫＰｍ１と対をなすメモリカード１１０固有の秘密復号鍵Ｋｍ１によって復号するための復号処理部１４２２と、禁止クラスリストのバージョン更新のためのデータＣＲＬ＿ｄａｔによって逐次更新される禁止クラスリストデータＣＲＬをバスＢＳ４より受けて格納するとともに、暗号化コンテンツデータ{Ｄａｔａ}Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆをバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１４１５は、禁止クラスリストＣＲＬを記録したＣＲＬ領域１４１５Ａと、コンテンツＩＤを含むＨｅａｄｅｒ、暗号化コンテンツデータ{Ｄａｔａ}Ｋｃ、および暗号化コンテンツデータの関連情報Ｄａｔａ－ｉｎｆを記録したデータ領域１４１５Ｂとから成る。

【０１２０】メモリカード１１０は、さらに、復号処理部１４２２によって得られるライセンスを保持するためのライセンス情報保持部１４４０と、バスＢＳ３を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【０１２１】ライセンス情報保持部１４４０は、Ｎ個（Ｎ：自然数）のバンクを有し、各ライセンスに対応するライセンスをバンクごとに保持する。

【０１２２】なお、図７において、実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）である。

【０１２３】もちろん、メモリ１４１５も含めて、モジュールＴＲＭ内に組込まれる構成としてもよい。しかしながら、図７に示したような構成とすることで、メモリ１４１５中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１５中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１５を設ける必要がないので、製造コストが低減されるという利点がある。

【０１２４】図８～図１１は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第１～第４のフローチャートである。

【０１２５】図８を参照して、携帯電話機１００のユーザからキー操作部１１０８を介してコンテンツデータの配信要求がなされると、携帯電話機１００は、メニューの送信要求を配信サーバ３０へ送信する（ステップＳ７０）。配信サーバ３０の配信制御部３１５は、通信装置３５０およびバスＢＳ１を介してメニューの送信要求を受信すると（ステップＳ７２）、メニューデータベース３０７からバスＢＳ１を介してメニューを読出し、その読出したメニューをバスＢＳ１および通信装置３５０を介して携帯電話機１００へ送信する（ステップＳ７４）。携帯電話機１１０は、送受信部１１０４によってメニューを受信し、コントローラ１１０６は、メニューを表示部１１１０に表示する（ステップＳ７６）。

【０１２６】そうすると、携帯電話機１００の表示部１１１０には、図１２に示すメニュー６１が表示される。ユーザは、メニュー６１の選択番号１，２，３，・・・を選択することによって配信を希望する暗号化コンテンツデータのジャンルを選択する。表示部１１１０には、別の画面に移行するための移行部１１１１が設けられている。ユーザは、表示部１１１０に表示されたメニュー６１から希望する暗号化コンテンツデータのジャンルを選択すると、移行部１１１１をクリックする。

【０１２７】携帯電話機１００のコントローラ１１０６は、ジャンルが選択された否かを判断する（ステップＳ７８）。選択すべきジャンルが存在しないときはステップＳ１７０へ移行し、配信動作は終了する。ジャンルが選択され、移行部１１１１がクリックされると、コントローラ１１０６は、選択されたジャンルに含まれるアド

レスを送受信部１１０４を介して配信サーバ３０へ送信し、選択されたジャンルの画面を送信するように要求する（ステップＳ８０）。メニュー６１から「地域関連」のジャンルが選択されると、携帯電話機１００のコントローラ１１０６は、地域関連のアドレスを送受信部１１０４を介して配信サーバ３０へ送信する。

【０１２８】配信サーバ３０の配信制御部３１５は、通信装置３５０およびバスＢＳ１を介してジャンルメニューの送信要求を受信すると（ステップＳ８１）、メニューデータベース３０７からバスＢＳ１を介して要求されたジャンルメニューを読出し、その読出したジャンルメニューをバスＢＳ１および通信装置３５０を介して携帯電話機１００へ送信する（ステップＳ８２）。地域関連のジャンルを要求された場合、配信制御部３１５は、地域関連のジャンルに含まれるメニューをメニューデータベース３０７から読出し、バスＢＳ１および通信装置３５０を介して携帯電話機１００へ送信する。

【０１２９】携帯電話機１１０は、送受信部１１０４によってジャンルメニューを受信し、コントローラ１１０６は、ジャンルメニューを表示部１１１０に表示する（ステップＳ８３）。そうすると、携帯電話機１００の表示部１１１０には、図１２に示すジャンルメニュー６２が表示される。ユーザは、ジャンルメニュー６２の選択番号１，２，３，・・・を選択することによって配信を希望する暗号化コンテンツデータの項目を選択する。ユーザが選択した地域関連のジャンルメニュー６２は、曲名、歌詞、出身歌手、出身作曲者等から成る。地域関連のジャンルメニュー６２に含まれる曲名、歌詞、出身歌手、出身作曲者等は、携帯電話機１００の現在位置の地名を含む曲名、歌詞、その地名を出身地とする歌手、作曲者等を表す。たとえば、携帯電話機１００の現在位置が東京であるならば、曲名に「東京」を含む音楽データを意味する。この地名の範囲は、そう狭い地域を指すのではなく、おおむね都道府県程度である。

【０１３０】ユーザは、ディスプレイ１１１０を見て表示された地域関連のジャンルメニュー６２から希望する項目を選択し、移行部１１１１をクリックする。携帯電話機１００のコントローラ１１０６は、項目が選択された否かを判断する（ステップＳ８４）。選択すべき項目が存在しないときはステップＳ１７０へ移行し、配信動作は終了する。項目が選択され、移行部１１１１がクリックされると、コントローラ１１０６は、選択された項目に含まれるアドレスを送受信部１１０４を介して配信サーバ３０へ送信し、選択された項目の画面を送信するように要求するとともに、位置検出部１２２６がＧＰＳによって検出した携帯電話機１００の現在位置を送信する（ステップＳ８５）。ジャンルメニュー６２から「曲名」の項目が選択されると、携帯電話機１００のコントローラ１１０６は、曲名のアドレスを送受信部１１０４を介して配信サーバ３０へ送信する。

【０１３１】配信サーバ３０の配信制御部３１５は、通信装置３５０およびバスＢＳ１を介して項目メニューの送信要求および携帯電話機１００の現在位置を受信する（ステップＳ８６）。そして、配信制御部３１５は、バスＢＳ１を介して情報データベース３０４から携帯電話機１００の現在位置が所在する地名を曲名に含む音楽データを検索し、その曲名リストを読出し、バスＢＳ１および通信装置３５０を介して携帯電話機１００へ送信する（ステップＳ８７）。携帯電話機１００の現在位置が所在する地名が東京であるならば、配信制御部３１５は、東京を曲名に含む音楽データの曲名リストを携帯電話機１００に送信する。

【０１３２】携帯電話機１００のコントローラ１１０６は、送受信部１１０４を介して曲名リストを受信し、ディスプレイ１１１０に曲名リスト６３を表示する（ステップＳ８３）。ユーザは、ディスプレイ１１１０に表示された曲名リスト６３を見て表示された曲名リスト６３から希望する曲を選択する。

【０１３３】携帯電話機１００のコントローラ１１０６は、曲名が選択された否かを判断する（ステップＳ８９）。選択すべき曲名がないときは、ステップＳ１７０へ移行し、配信動作は終了する。

【０１３４】曲名リスト６３は、暗号化コンテンツデータを特定するためのコンテンツＩＤを含んでおり、ステップＳ８９において暗号化コンテンツデータが選択されたとき、曲名リスト６３から選択された暗号化コンテンツデータのコンテンツＩＤが抽出される（ステップＳ９０）。そして、キー操作部１１０８を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ９１）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータの再生回数制限ＡＣ１、および再生期限ＡＣ２を設定して購入条件ＡＣが入力される。

【０１３５】他のジャンル、および項目が選択されたときも、上記と同じ方法によって選択されたジャンル、および項目が配信サーバ３０から携帯電話機１００に送信され、最終的に、ユーザが希望する暗号化コンテンツデータが特定される。

【０１３６】また、曲名リスト６３から暗号化音楽データを最終的に決定するとき、配信サーバ３０と接続した状態で、配信サーバ３０で再生された音楽データを携帯電話機１００が受信し、ユーザが試聴した後に配信を希望する暗号化音楽データを最終的に決定するようにしても良い。

【０１３７】次に、図９を参照して、携帯電話機１００は、ユーザが暗号化コンテンツデータを選択することによって抽出したコンテンツＩＤ（ステップＳ９０参照）の指定による配信リクエストがなされる（ステップＳ１００）。

【０１３８】メモリカード１１０においては、この配信リクエストに応じて、認証データ保持部１４００より認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａが出力される（ステップＳ１０２）。

【０１３９】携帯電話機１００は、メモリカード１１０からの認証のための認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣとを配信サーバ３０に対して送信する（ステップＳ１０４）。

【０１４０】配信サーバ３０では、携帯電話機１００からコンテンツＩＤ、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａ、ライセンス購入条件のデータＡＣを受信し（ステップＳ１０６）、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰｍａで復号処理を実行する（ステップＳ１０８）。

【０１４１】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからの公開暗号鍵ＫＰｍｃ１と証明書Ｃｍｃ１を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１０）。正当な認証データであると判断された場合、配信制御部３１５は、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を承認し、受理する。そして、次の処理（ステップＳ１１２）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を受理しないで処理を終了する（ステップＳ１７０）。

【０１４２】認証の結果、正規の機器であることが認識されると、配信制御部３１５は、次に、メモリカード１１０のクラス証明書Ｃｍｃ１が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１７０）。

【０１４３】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１２）。

【０１４４】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ３０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ１１３）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵ＫＰｍｃ１によって、暗号処理部３１８によって暗号化される（ステップＳ１１４）。

【０１４５】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍｃ１として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１１６）。

【０１４６】携帯電話機１００が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍｃ１を受信すると（ステップＳ１１８）、メモリカード１１０においては、メモリインタフェース１２００を介して、バスＢＳ３に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵Ｋｍｃ１により復号処理することにより、セッションキーＫｓ１を復号し抽出する（ステップＳ１２０）。

【０１４７】コントローラ１４２０は、配信サーバ３０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対して、メモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。

【０１４８】また、配信セッションにおいては、コントローラ１４２０は、メモリカード１１０内のメモリ１４１５に記録されている禁止クラスリストのデータＣＲＬ＿ｄａｔをメモリ１４１５から抽出してバスＢＳ４に出力する。

【０１４９】暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４０４より与えられるセッションキーＫｓ１によって、切換スイッチ１４４４および１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、公開暗号鍵ＫＰｍ１および禁止クラスリストのデータＣＲＬ＿ｄａｔを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ１をバスＢＳ３に出力する（ステップＳ１２２）。

【０１５０】バスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１は、バスＢＳ３からインタフェース１４２３、端子１２０１およびメモリインタフェース１２００を介して携帯電話機１００に出力され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ１２４）。

【０１５１】配信サーバ３０は、トランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、メモリカード１１０固有の公開暗号鍵ＫＰｍ１およびメモリカード１１０における禁止クラスリストのデータＣＲＬ＿ｄａｔを受理する（ステップＳ１２６）。

【０１５２】配信制御部３１５は、ステップＳ１０６で取得したコンテンツＩＤおよびライセンス購入条件のデータＡＣに従って、ライセンスＩＤ、アクセス制限情報

ＡＣ１および再生期限ＡＣ２を生成する（ステップＳ１２８）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ１３０）。

【０１５３】配信制御部３１５は、生成したライセンス、すなわち、ライセンス鍵Ｋｃ、再生期限ＡＣ２、ライセンスＩＤ、コンテンツＩＤ、およびアクセス制限情報ＡＣ１を暗号処理部３２６に与える。暗号処理部３２６は、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵ＫＰｍ１によってライセンスを暗号化する（ステップＳ１３２）図１０を参照して、配信サーバ３０において、メモリカード１１０から送信された禁止クラスリストのデータＣＲＬ＿ｄａｔが最新か否かが判断され、データＣＲＬ＿ｄａｔが最新と判断されたとき、ステップＳ１３４へ移行する。また、データＣＲＬ＿ｄａｔが最新でないときはステップＳ１３７へ移行する（ステップＳ１３３）。

【０１５４】データＣＲＬ＿ｄａｔが最新と判断されたとき、暗号処理部３２８は、暗号処理部３２６から出力された暗号化データ｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１をメモリカード１１０において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１｝Ｋｓ２をバスＢＳ１に出力する。そして、配信制御部３１５は、バスＢＳ１上の暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１｝Ｋｓ２を通信装置３５０を介して携帯電話機１００へ送信する（ステップＳ１３４）。

【０１５５】そして、携帯電話機１００は、暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１｝Ｋｓ２を受信し（ステップＳ１３５）、バスＢＳ２およびメモリインタフェース１２００を介してメモリカード１１０へ送信する。メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１｝Ｋｓ２を端子１２０１およびインタフェース１４２３を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１を受理する（ステップＳ１３６）。その後、ステップＳ１４６へ移行する。

【０１５６】一方、配信サーバ３０において、ＣＲＬ＿ｄａｔが最新でないと判断されると、配信制御部３１５は、バスＢＳ１を介してＣＲＬデータベース３０６から最新の禁止クラスリストのデータＣＲＬ＿ｄａｔを取得する（ステップＳ１３７）。

【０１５７】暗号処理部３２８は、暗号処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する禁止クラスリストの最新データＣＲＬ＿ｄａｔとを受けて、メモリカード１１０において生成されたセッションキーＫｓ２によって暗号化する。暗号処理部３２８より出力された暗号化データは、バスＢＳ１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１３８）。

【０１５８】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１５９】携帯電話機１００は、送信された暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ２を受信し（ステップＳ１４０）、メモリインタフェース１２００を介してメモリカード１１０へ出力する。メモリカード１１０においては、端子１２０１およびインタフェース１４２３を介して、バスＢＳ３に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ３の受信データを復号しバスＢＳ４に出力する（ステップＳ１４２）。

【０１６０】この段階で、バスＢＳ４には、Ｋｍ１保持部１４２１に保持される秘密復号鍵Ｋｍ１で復号可能な暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１と、ＣＲＬ＿ｄａｔとが出力される（ステップＳ１４２）。コントローラ１４２０の指示によって受理した最新の禁止クラスリストＣＲＬ＿ｄａｔによってメモリ１４１５内の禁止クラスリストＣＲＬが書き換えられる（ステップＳ１４４）。

【０１６１】ステップＳ１３４，Ｓ１３５，Ｓ１３６は、メモリカード１１０から送られてきた禁止クラスリストＣＲＬ＿ｄａｔが最新の場合のライセンス鍵Ｋｃ等のメモリカード１１０への配信動作であり、ステップＳ１３７，Ｓ１３８，Ｓ１４０，Ｓ１４２，Ｓ１４４は、メモリカード１１０から送られてきた禁止クラスリストＣＲＬ＿ｄａｔが最新でない場合のライセンス鍵Ｋｃ等のメモリカード１１０への配信動作である。このように、メモリカード１１０から送られてきた禁止クラスリストＣＲＬ＿ｄａｔが更新されているか否かを、逐一、確認し、更新されていないとき、最新の禁止クラスリストＣＲＬ＿ｄａｔをＣＲＬデータベース３０６から取得し、メモリカード１１０に配信することによって、ライセンスの破られたメモリカードへの暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信を防止し、かつ、ライセンスの破られた携帯電話機による暗号化コンテンツデータ

{Ｄａｔａ}Ｋｃの再生を防止できる。

【０１６２】ステップＳ１３６またはステップＳ１４４の後、コントローラ１４２０の指示によって、暗号化ライセンス{Ｋｃ//ＡＣ２//ライセンスＩＤ//コンテンツＩＤ//ＡＣ１}Ｋｍ１は、復号処理部１４２２において、秘密復号鍵Ｋｍ１によって復号され、ライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、再生回数制限ＡＣ１および再生期限ＡＣ２）が受理される（ステップＳ１４８）。

【０１６３】コントローラ１４２０は、ライセンスをライセンス情報保持部１４４０に記録する（ステップＳ１５０）。

【０１６４】図１１を参照して、携帯電話機１００のコントローラ１１０６は、ステップＳ８８およびステップＳ９４において立てたフラグを参照し、配信サーバ３０から暗号化コンテンツデータを取得するか否かを判断する。そして、暗号化コンテンツデータを配信サーバ３０から取得しないとき、ステップＳ１６４へ移行し、暗号化コンテンツデータを配信サーバ３０から取得するとき、ステップＳ１５４へ移行する。

【０１６５】暗号化コンテンツデータを配信サーバ３０から取得するとき、携帯電話機１００は、配信サーバ３０から送られたトランザクションＩＤと、暗号化コンテンツデータの配信要求を配信サーバ３０へ送信する（ステップ１５４）。

【０１６６】配信サーバ３０は、トランザクションＩＤおよび暗号化コンテンツデータの配信要求を受信し（ステップＳ１５６）、情報データベース３０４より、暗号化コンテンツデータ{Ｄａｔａ}Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１５８）。

【０１６７】携帯電話機１００は、{Ｄａｔａ}Ｋｃ//Ｄａｔａ－ｉｎｆを受信して、暗号化コンテンツデータ{Ｄａｔａ}Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを受理する（ステップＳ１６０）。暗号化コンテンツデータ{Ｄａｔａ}Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆは、メモリインタフェース１２００、端子１２０１、およびインタフェース１４２３を介してメモリカード１１０のバスＢＳ３に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ{Ｄａｔａ}Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆがそのままメモリ１４１５に記録される（ステップＳ１６２）。

【０１６８】そして、ステップＳ１５２において暗号化コンテンツデータを配信サーバ３０から受信しないと判断されたときも含め、メモリカード１１０から配信サーバ３０へは、トランザクションＩＤ//配信受理の通知が送信され（ステップＳ１６４）、配信サーバ３０でトランザクションＩＤ//配信受理を受信すると（ステップＳ１６６）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行われて配信終了の処理が実行され（ステップＳ１６８）、全体の処理が終了する（ステップＳ１７０）。

【０１６９】このようにして、携帯電話機１００に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍｃ１とともに暗号化して送信できた公開暗号鍵ＫｐｌおよびＫｍｃ１が有効であることを確認した上で、それぞれのクラス証明書Ｃｍｃ１が禁止クラスリスト、すなわち、公開暗号鍵ＫｐｌおよびＫｍｃ１による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０１７０】また、配信サーバ３０への暗号化コンテンツデータ{Ｄａｔａ}Ｋｃの配信要求時にメモリカード１１０における暗号化コンテンツデータ{Ｄａｔａ}Ｋｃ、ライセンス鍵Ｋｃ、および再生回数制限ＡＣ１等の記録状況に応じて、必要な配信だけを配信サーバ３０に要求することができる。その結果、無駄な配信を防止することができる。

【０１７１】次に、図１３および図１４を参照してメモリカード１１０に配信されたコンテンツデータの携帯電話機１００における再生動作について説明する。図１３を参照して、再生動作の開始とともに、携帯電話機１００のユーザからキー操作部１１０８を介して再生指示が携帯電話機１００にインプットされる（ステップＳ２００）。そうすると、コントローラ１１０６は、バスＢＳ２を介して認証データ保持部１２０２から認証データ{ＫＰｐ１//Ｃｒｔｆ１}ＫＰｍａを読出し、メモリインタフェース１２００を介してメモリカード１１０へ認証データ{ＫＰｐ１//Ｃｒｔｆ１}ＫＰｍａを入力する（ステップＳ２０１）。

【０１７２】そうすると、メモリカード１１０は、認証データ{ＫＰｐ１//Ｃｒｔｆ１}ＫＰｍａを受理する（ステップＳ２０２）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ{ＫＰｐ１//Ｃｒｔｆ１}ＫＰｍａを、ＫＰｍａ保持部１４１４に保持された公開認証鍵ＫＰｍａによって復号し（ステップＳ２０３）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ{ＫＰｐ１//Ｃｒｔｆ１}ＫＰｍａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ２０４）。復号できなかった場合、コントローラ１４２０は認証データ不受理の出力をデータＢＳ３および端子１２０１を介して携帯電話機１００のメモリインタフェース１２００へ出力する（ステップＳ２０６）。認証データが復号できた場合、コントローラ１４２０は、取得した証明書Ｃｒｔｆ１がメモリ

１４１５から読出した禁止クラスリストデータに含まれるか否かを判断する（ステップＳ２０５）。この場合、証明書Ｃｒｔｆ１にはＩＤが付与されており、コントローラ１４２０は、受理した証明書Ｃｒｔｆ１のＩＤが禁止クラスリストデータの中に存在するか否かを判別する。証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれると判断されると、コントローラ１４２０は認証データ不受理の出力をデータＢＳ３および端子１２０１を介して携帯電話機１００のメモリインタフェース１２００へ出力する（ステップＳ２０６）。

【０１７３】ステップＳ２０４において認証データが公開認証鍵ＫＰｍａで復号できなかったとき、およびステップＳ２０５において受理した証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して認証データ不受理の出力を受けると、認証データ不受理のデータをディスプレイ１１１０に表示する（ステップＳ２０７）。

【０１７４】ステップＳ２０５において、証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれていないと判断されると、図１４を参照して、メモリカード１１０のセッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ２０８）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する（ステップＳ２０９）。そうすると、コントローラ１４２０は、端子１２０１を介してメモリインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力し、携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、Ｋｐ１保持部１２０４は、秘密復号鍵Ｋｐ１を復号処理部１２０６へ出力する。

【０１７５】復号処理部１２０６は、Ｋｐ１保持部１２０４から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１２０８へ出力する（ステップＳ２１０）。そうすると、セッションキー発生部１２１０は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１２０８へ出力する（ステップＳ２１１）。暗号処理部１２０８は、セッションキー発生部１２１０からのセッションキーＫｓ３を復号処理部１２０６からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、コントローラ１１０６は、バスＢＳ２およびメモリインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ２１２）。

【０１７６】メモリカード１１０の復号処理部１４１２は、端子１２０１、インタフェース１４２３、およびバスＢＳ３を介して｛Ｋｓ３｝Ｋｓ２を入力し、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、携帯電話機１００で発生されたセッションキーＫｓ３を取得する（ステップＳ２１３）。

【０１７７】セッションキーＫｓ３の受理に応じて、コントローラ１４２０は、ライセンス情報保持部１４４０内の対応するアクセス制限情報ＡＣ１を確認する（ステップＳ２１４）。

【０１７８】ステップＳ２１４においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数制限に制限がある場合にはアクセス制限情報ＡＣ１のデータを更新し再生可能回数を更新した後に次のステップに進む（ステップＳ２１５）。一方、アクセス制限情報ＡＣ１によって再生回数制限が制限されていない場合においては、ステップＳ２１５はスキップされ、再生回数制限ＡＣ１は更新されることなく処理が次のステップ（ステップＳ２１６）に進行される。

【０１７９】また、ライセンス情報保持部１４４０内にリクエスト曲の当該コンテンツＩＤが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【０１８０】ステップＳ２１４において、当該再生動作において再生が可能であると判断された場合には、ライセンス情報保持部１４４０に記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生期限ＡＣ２がバスＢＳ４上に出力される（ステップＳ２１６）。

【０１８１】得られたライセンス鍵Ｋｃと再生期限ＡＣ２は、切換スイッチ１４４４の接点Ｐｄを介して暗号処理部１４０６に送られる。暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐｄを介して復号処理部１４１２より受けたセッションキーＫｓ３によってバスＢＳ４から受けたライセンス鍵Ｋｃと再生期限ＡＣ２とを暗号化し、｛Ｋｃ／／ＡＣ２｝Ｋｓ３をバスＢＳ３に出力する（ステップＳ２１７）。

【０１８２】バスＢＳ３に出力された暗号化データは、インタフェース１４２３、端子１２０２、およびメモリインタフェース１２００を介して携帯電話機１００に送出される。

【０１８３】携帯電話機１００においては、メモリインタフェース１２００を介してバスＢＳ２に伝達される暗号化データ｛Ｋｃ／／ＡＣ２｝Ｋｓ３を復号処理部１２１２によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生期限ＡＣ２を受理する（ステップＳ２１８）。復号処理部１２１２は、ライセンス鍵Ｋｃを復号処理部１２１４に伝達し、再生期限ＡＣ２をバスＢＳ２に出力す

る。

【０１８４】コントローラ１１０６は、バスＢＳ２を介して、再生期限ＡＣ２を受理して再生の可否の確認を行なう（ステップＳ２１９）。

【０１８５】ステップＳ２１９においては、再生期限ＡＣ２によって再生不可と判断される場合には、再生動作は終了される。

【０１８６】ステップＳ２１９において再生可能と判断された場合、コントローラ１１０６は、メモリインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、バスＢＳ３および端子１２０１を介してメモリインタフェース１２００へ出力する（ステップＳ２２０）。

【０１８７】携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、バスＢＳ２を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１４へ与える。そして、復号処理部１２１４は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１２から出力されたコンテンツ鍵Ｋｃによって復号してコンテンツデータＤａｔａを取得する（ステップＳ２２１）。

【０１８８】そして、復号されたコンテンツデータＤａｔａは音楽再生部１２１６へ出力され、音楽再生部１２１６は、コンテンツデータを再生し、ＤＡ変換器１２１８はディジタル信号をアナログ信号に変換して端子１２２０へ出力する。そして、スイッチ１２２２は端子１２２０を選択して音楽データは端子１２２４を介してヘッドホーン１３０へ出力されて再生される（ステップＳ２２２）。これによって再生動作が終了する。

【０１８９】上記においては、携帯電話機１００は、現在位置をＧＰＳによって検出し、その検出した現在位置を配信サーバ３０へ送信するとして説明したが、本発明においては、これに限らず、配信サーバ３０は、他の方法によって携帯電話機１００の現在位置を取得しても良い。すなわち、配信サーバ３０は、図１５に示す位置情報センター４０から携帯電話機１００の現在位置を取得しても良い。配信サーバ３０は、位置情報センター４０と接続されている。位置情報センター４０は、地図データベース４１、基地局データベース４２、および端末機位置データ４３を含む。位置情報センター４０は、電話網５０と接続されており、電話網５０は、公衆回線網５１と、基地局５２～５４とを含む。

【０１９０】配信サーバ３０は、携帯電話機１００から暗号化コンテンツデータの配信要求を受信すると、位置情報センター４０に携帯電話機１００の現在位置を要求する。そうすると、位置情報センター４０は、基地局５２～５４の基地局データを電話網５０に要求する。基地局５２～５４は、公衆回線網５１を介して基地局データの要求を受取り、携帯電話機１００に基地局データを要求する。

【０１９１】携帯電話機１００は、基地局コードと電界強度情報とを基地局５２～５４へ送信する。そして、基地局５２～５４は、基地局コードと電界強度情報とを公衆回線網５１を介して位置情報センター４０へ送信する。位置情報センター４０は、受信した基地局コードに基づいて基地局データベース４２を検索し、基地局コードと電界強度情報とを送信してきた３つの基地局の所在地を抽出する。また、位置情報センター４０は、受信した電界強度情報に基づいて、携帯電話機１００が３つの基地局５２～５４からどの程度離れているかを計算する。そして、位置情報センター４０は、３つの基地局の所在地、および３つの基地局からの距離に基づいて、地図データベース４１を参照して携帯電話機１００の現在位置を割出し、その割出した現在位置を配信サーバ３０へ送信するとともに端末機位置データベース４３に記憶する。

【０１９２】これによって、配信サーバ３０は、暗号化コンテンツデータの配信を要求した携帯電話機１００の現在位置を検知することができる。

【０１９３】携帯電話機１００が配信サーバ３０へ携帯電話網を介して暗号化コンテンツデータの配信を要求するので、携帯電話機１００は暗号化コンテンツデータの配信要求と同時に基地局コードを配信サーバへ送信するようにしても良い。配信サーバ３０は、基地局コードに対応する地名データベースを保持しており、受信した基地局コードに基づいて携帯電話機１００の現在位置が所在する地名を割出すことができる。本発明において要求される現在位置に関する位置情報は、都道府県レベルの位置情報でよいので、配信サーバ３０は基地局コードに基づいて位置情報を得ることができる。

【０１９４】また、本発明においては、コンサート会場近くで配信サーバ３０へ暗号化コンテンツデータの配信要求を行なったとき、そのコンサート会場で演奏されている音楽データを携帯電話機１００へ送信するようにしても良い。携帯電話機１００の現在位置の検出方法は上述したのと同じ方法である。この場合、配信サーバ３０は、配信要求された暗号化コンテンツデータのライセンスを携帯電話機１００へ送信する際、通常よりも安い料金を課金する。これによって、コンサート会場に入れなくても、コンサート会場で演奏されている音楽データを携帯電話機１００によって通常よりも安い料金で受信して聴くことができる。

【０１９５】さらに、本発明においては、配信サーバは、暗号化音楽データを携帯電話機１００へ配信する際、位置情報に関連する画像データも一緒に配信しても良い。この画像データは、携帯電話機１００の現在位置

が所在する地方の景色等である。携帯電話機１００は、受信した画像データをディスプレイ１１１０に表示し、音楽を聴きながら、その地方の景色を楽しむことができる。

【０１９６】また、さらに、上記においては、配信サーバ３０は携帯電話機１００の現在位置を受信してから、その位置情報に関連する暗号化コンテンツデータの検索をするとして説明したが、配信サーバ３０は、予め各位置情報に関連する暗号化コンテンツデータを分類して保持していても良い。

【０１９７】本発明の実施の形態によれば、携帯電話機は、現在位置に関連する暗号化コンテンツデータを受信し、音楽データを聴くことができるので、移動中に各地方に関連する音楽データを楽しむことができる。

【０１９８】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図５】　ライセンスサーバの構成を示す概略ブロック図である。

【図６】　携帯電話機の構成を示すブロック図である。

【図７】　メモリカードの構成を示すブロック図である。

【図８】　図１に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図９】　図１に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図１０】　図１に示すデータ配信システムにおける配信動作を説明するための第３のフローチャートである。

【図１１】　図１に示すデータ配信システムにおける配信動作を説明するための第４のフローチャートである。

【図１２】　配信サーバから携帯電話機に送信されたメニューを携帯電話機の表示部に表示した状態を示す図である。

【図１３】　携帯電話機における再生動作を説明するための第１のフローチャートである。

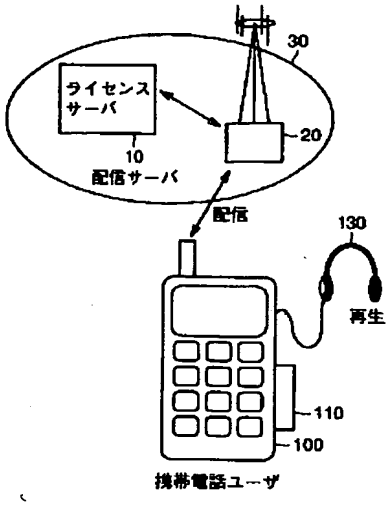
【図１４】　携帯電話機における再生動作を説明するための第２のフローチャートである。

【図１５】　携帯電話機の現在位置を検出するシステムを概念的に説明するための概略図である。

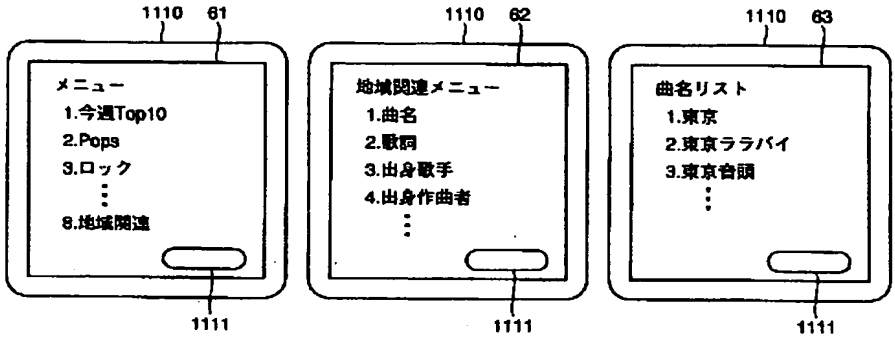
【符号の説明】

１０　ライセンスサーバ、２０　配信キャリア、３０　配信サーバ、４０　位置情報センター、４１　地図データベース、４２　基地局データベース、４３端末機位置データベース、５０　電話網、５１　公衆回線網、５２～５４　基地局、６１　メニュー、６２　ジャンルメニュー、６３　項目メニュー、１００携帯電話機、１１０　メモリカード、１３０　ヘッドホーン、１１０６，１４２０　コントローラ、３０２　課金データベース、３０４　情報データベース、３０６　ＣＲＬデータベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１２０６，１２１２，１２１４，１４０４，１４０８，１４１２，１４２２　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，１２１０，１４１８　セッションキー発生部、３１８，３２６，３２８，１２０８，１４０６，１４１０　暗号処理部、３５０　通信装置、１１０２　アンテナ、１１０４　送受信部、１１０８キー操作部、１１１０　ディスプレイ、１１１１　移行部、１１１２　音声再生部、１１１３，１２１８　ＤＡ変換器、１１１４，１２０１，１２２０，１２２４　端子、１１１５　マイク、１１１６　ＡＤ変換器、１１１７　音声符号化部、１２００　メモリインタフェース、１２０２，１４００　認証データ保持部、１２０４　Ｋｐ１保持部、１２１６　音楽再生部、１２２２　スイッチ、１４０２　Ｋｍｃ１保持部、１４１４　ＫＰｍａ保持部、１４１５　メモリ、１４１５Ａ　ＣＲＬ領域、１４１５Ｂ　データ領域、１４１６　ＫＰｍ１保持部、１４２１　Ｋｍ１保持部、１４２３　インタフェース、１４４０　ライセンス情報保持部、１４４２，１４４４，１４４６　切換スイッチ。

【図１】



【図１２】



【図２】

名称	属性	保持／発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ、アップデートプログラム
Kc	ライセンス鍵		暗号化コンテンツデータの復号鍵
(Data)Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータこの形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード（コンテンツIDを含めて識別することも可）
トランザクションID	ライセンス固有		配信を特定するための管理コード
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数,機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報（例：再生可否）

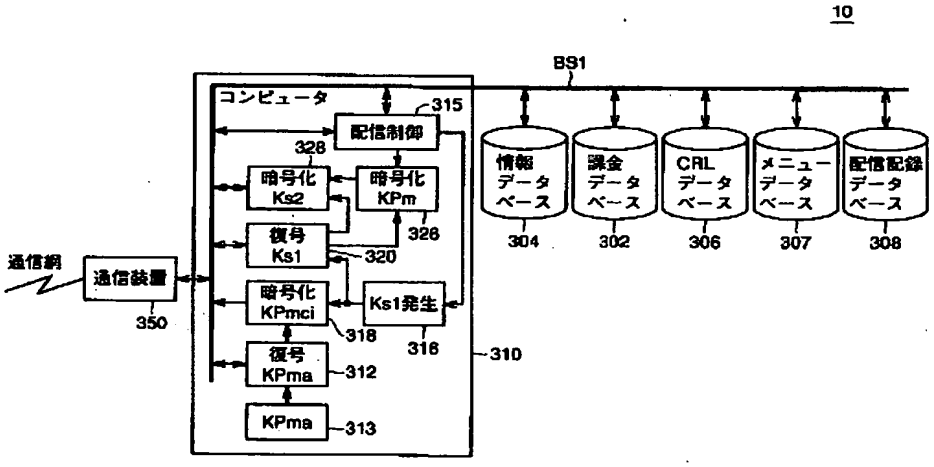
【図４】

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／再生セッション毎に発生
Ks3		携帯電話機	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 KPmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵（非対称鍵）	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開認証鍵	配信サーバ	配信システム全体で共通。

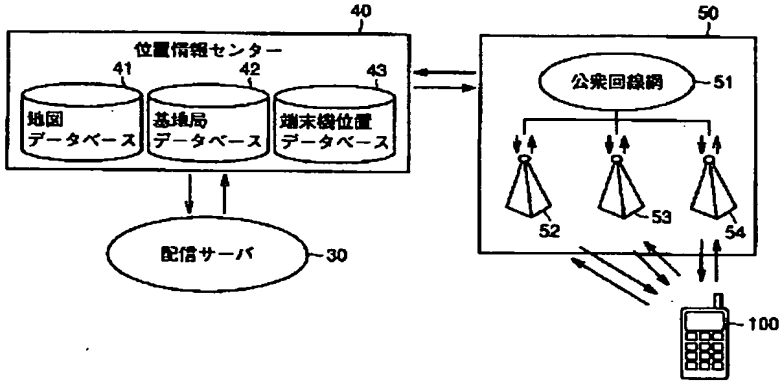
【図３】

名称	属性	保持／発生箇所	機能・特徴
CRL	禁止クラスリスト関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵 （非対称鍵）	携帯電話機	Kpnにて復号可能。 {KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊携帯電話機の種類nごとに異なる。
KPmci	公開暗号鍵 （非対称鍵）	メモリカード	Kmciにて復号可能。 {KPmci//Cmci}KPmaの形式で出荷時に記録 ＊メモリカードの種類iごとに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路（携帯電話機）固有の復号鍵 ＊携帯電話機の種類nごとに異なる。
Kmci	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 ＊メモリカードの種類iごとに異なる。
Crtfn	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 {KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊携帯電話機のクラスnごとに異なる。
Cmci		メモリカード	メモリカードのクラス証明書。認証機能を有する。 {KPmci//Cmci}KPmaの形式で出荷時に記録 ＊メモリカードのクラスiごとに異なる。

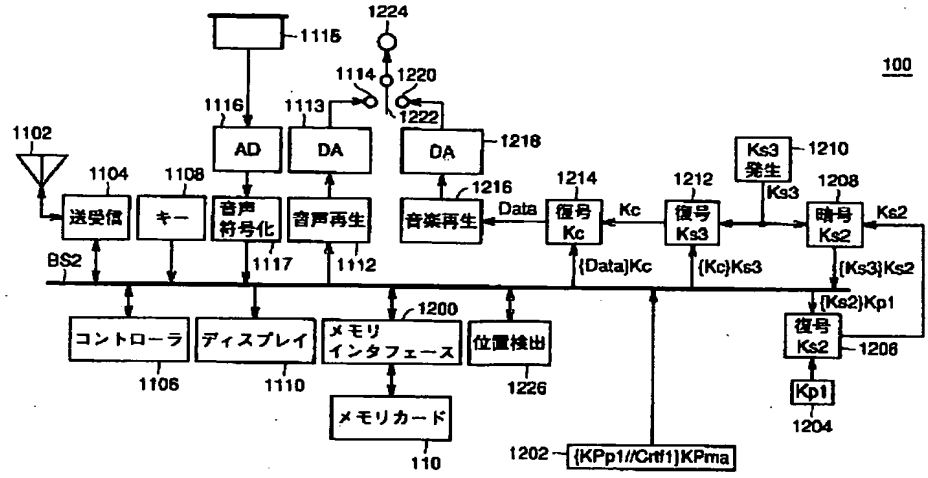
【図５】



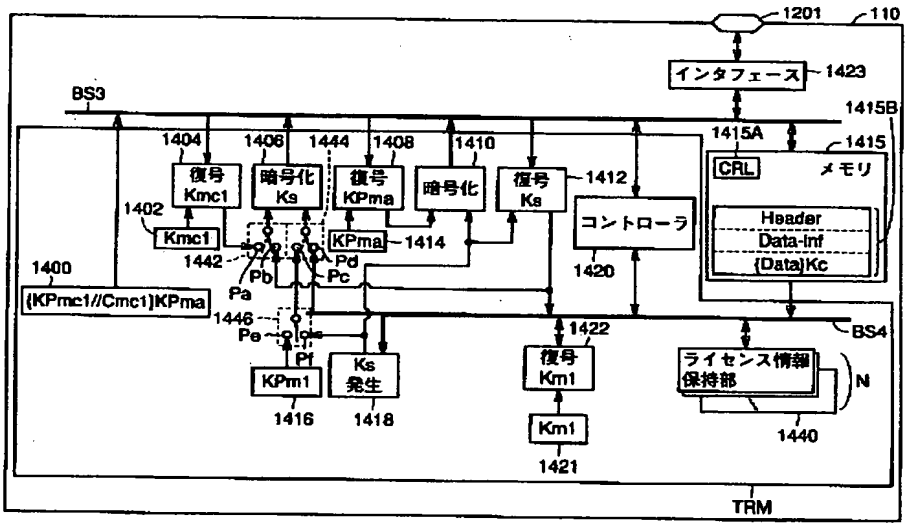
【図１５】



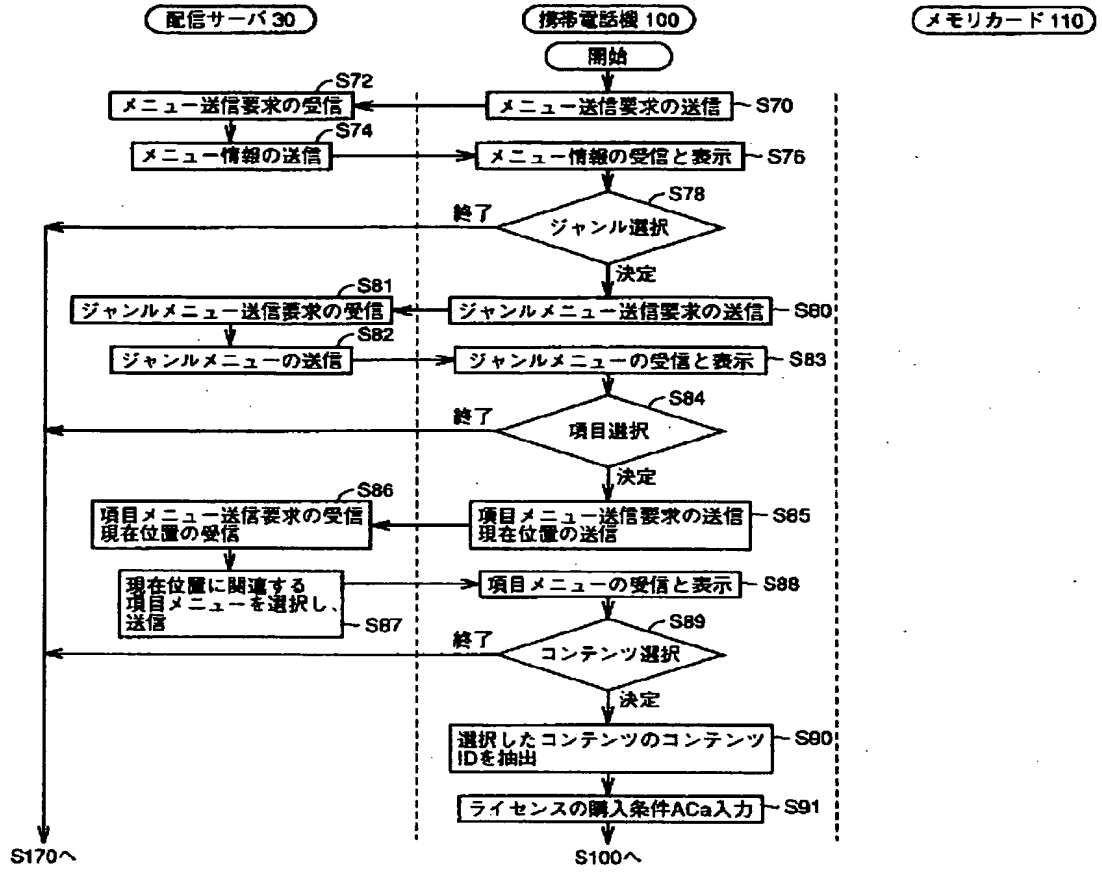
【図６】


100
1102
1104
1108
1116
1113
1114
1220
1222
1224
1115
AD
DA
DA
1218
1216
1214
1212
1210
1208
Ks3 発生
Ks3
送受信
キー
音声 符号化
音声再生
音楽再生
Data
復号 Kc
Kc
復号 Ks3
暗号 Ks2
Ks2
BS2
1117
1112
{Data}Kc
{Kc}Ks3
{Ks3}Ks2
{Ks2}Kp1
1200
コントローラ
ディスプレイ
メモリ インタフェース
位置検出
復号 Ks2
1206
1106
1110
1226
Kp1
1204
メモリカード
110
1202
{KPp1//Crtf1}KPma

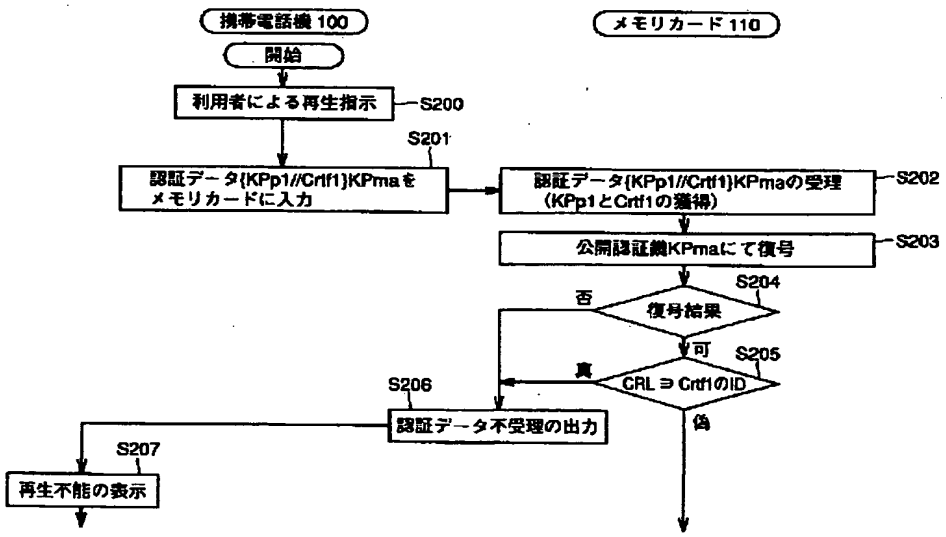
【図７】


1201
110
インタフェース
1423
BS3
1415B
1415A
1415
CRL
メモリ
1404
1406
1444
1408
1410
1412
復号 Kmc1
暗号化 Ks
復号 KPma
暗号化
復号 Ks
コントローラ
Header
Data-inf
{Data}Kc
1402
Kmc1
KPma
1414
1442
Pd
Pb
Pc
Pa
1420
1400
{KPmc1//Cmc1}KPma
1446
Pe
Pf
BS4
1422
復号 Km1
ライセンス情報 保持部
N
KPm1
Ks 発生
1416
1418
Km1
1421
1440
TRM

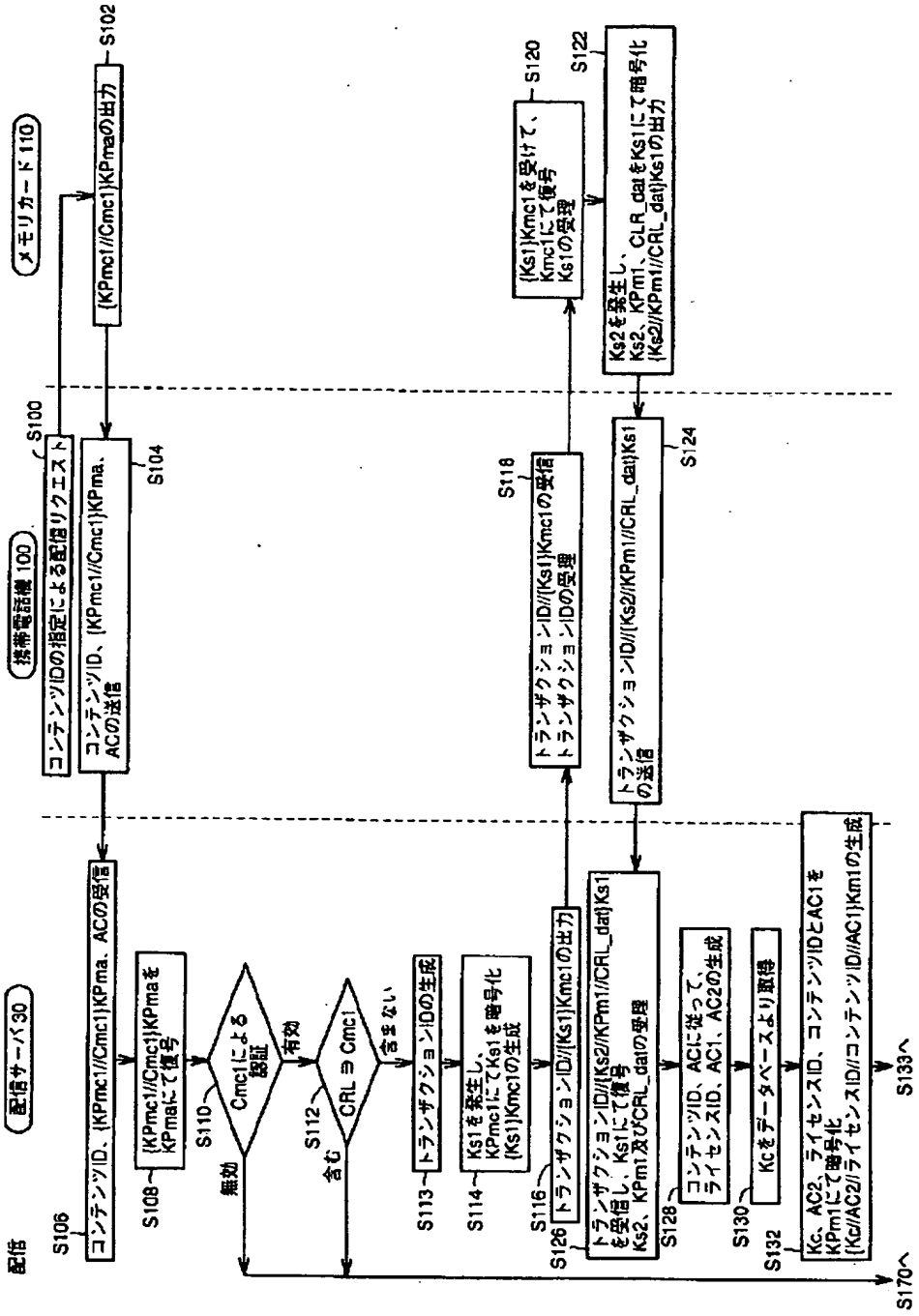
【図８】


配信サーバ30
携帯電話機100
メモリカード110
開始
S72
メニュー送信要求の受信
S70
メニュー送信要求の送信
S74
メニュー情報の送信
S75
メニュー情報の受信と表示
S78
終了
ジャンル選択
決定
S81
ジャンルメニュー送信要求の受信
S80
ジャンルメニュー送信要求の送信
S82
ジャンルメニューの送信
S83
ジャンルメニューの受信と表示
S84
終了
項目選択
決定
S86
項目メニュー送信要求の受信
現在位置の受信
S85
項目メニュー送信要求の送信
現在位置の送信
現在位置に関連する
項目メニューを選択し、
送信
S87
S88
項目メニューの受信と表示
S89
終了
コンテンツ選択
決定
選択したコンテンツのコンテンツ
IDを抽出
S90
ライセンスの購入条件ACa入力
S91
S170へ
S100へ

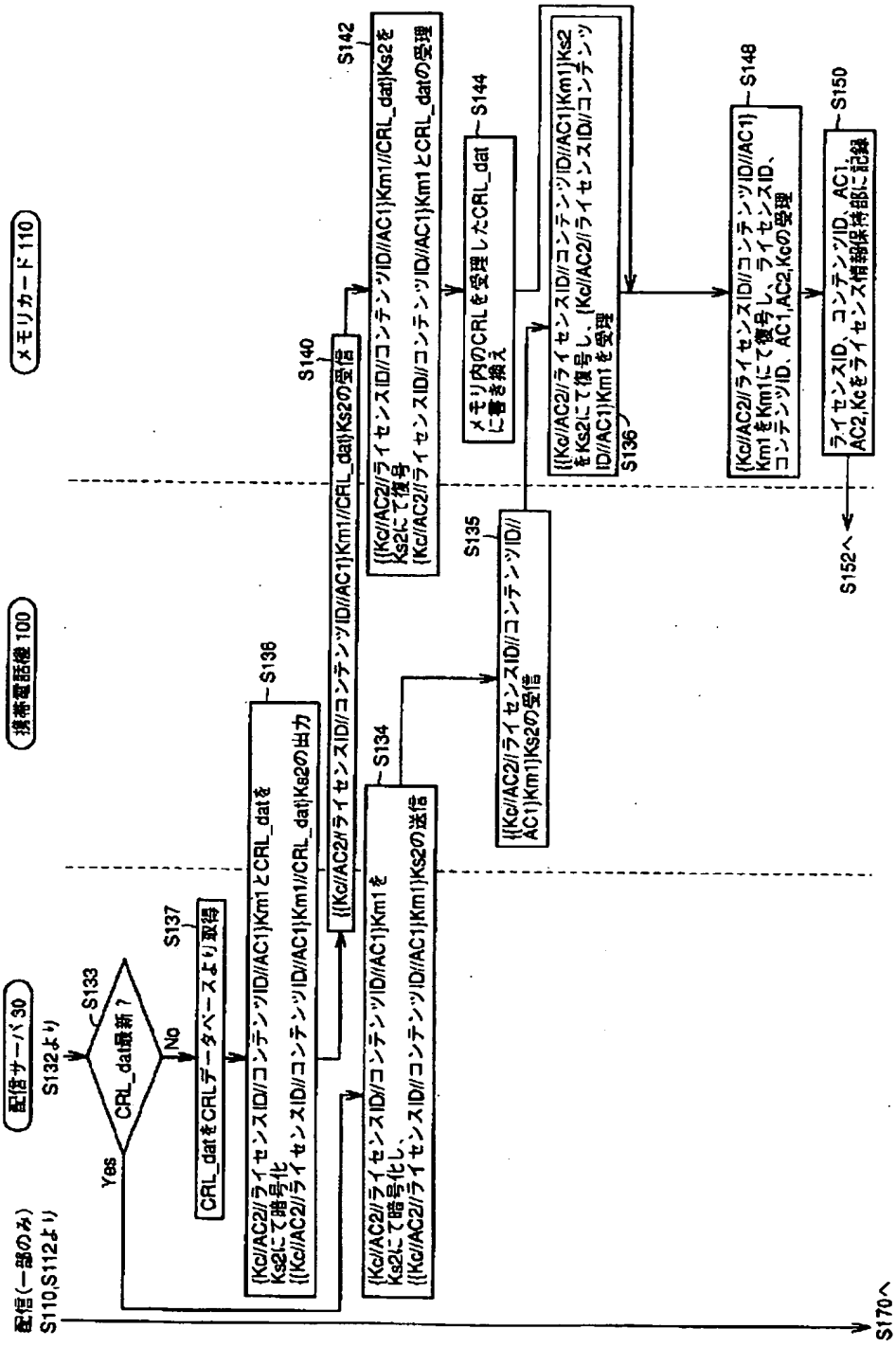
【図１３】


携帯電話機100
メモリカード110
開始
利用者による再生指示
S200
S201
認証データ{KPp1//Crtf1}KPmaを
メモリカードに入力
認証データ{KPp1//Crtf1}KPmaの受理
(KPp1とCrtf1の獲得)
S202
公開認証鍵KPmaにて復号
S203
S204
否
復号結果
可
S205
真
CRL ∋ Crtf1のID
S206
偽
認証データ不受理の出力
S207
再生不能の表示

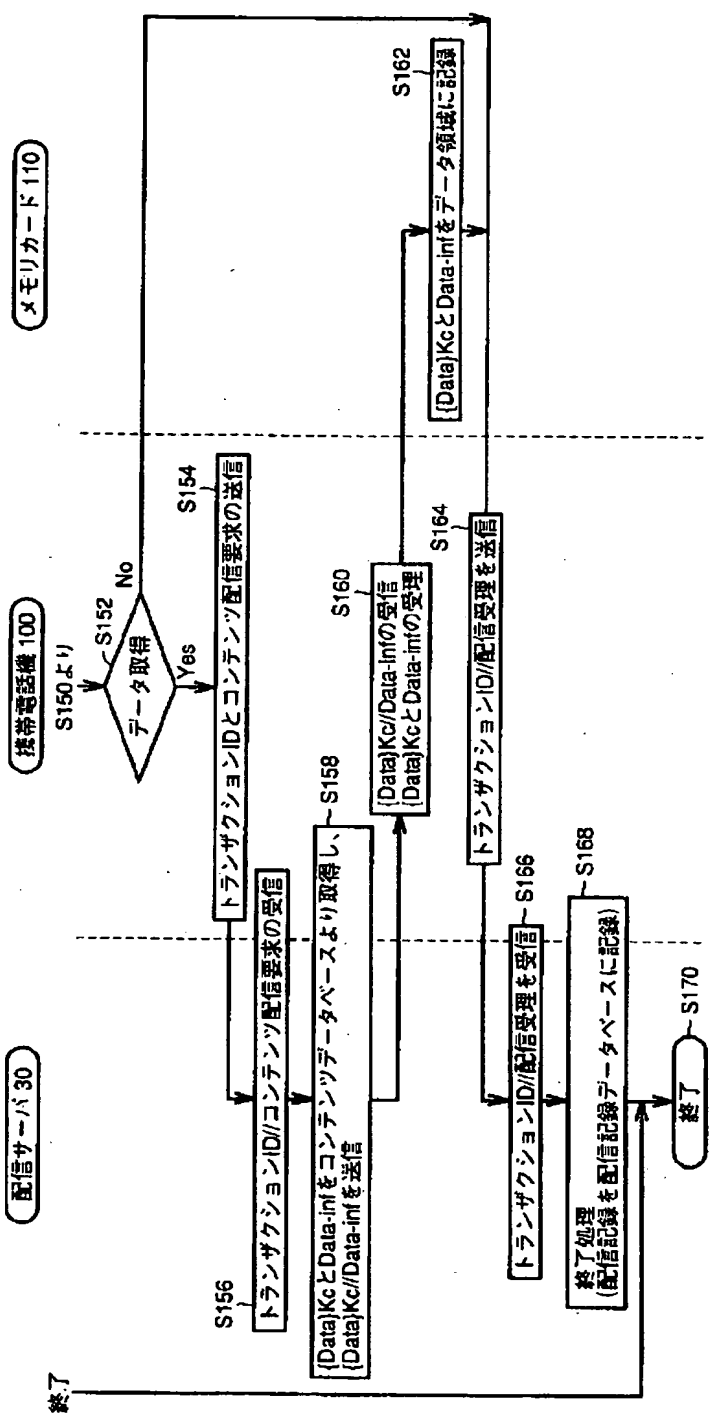
【図９】


メモリカード 110
携帯電話機 100
配信サーバ 30
配信
コンテンツIDの指定による配信リクエスト
S100
{KPmc1//Cmc1}KPmaの出力
S102
コンテンツID、{KPmc1//Cmc1}KPma、ACの送信
S104
コンテンツID、{KPmc1//Cmc1}KPma、ACの受信
S106
{KPmc1//Cmc1}KPmaをKPmaにて復号
S108
Cmc1による認証
S110
無効
有効
CRL ∋ Cmc1
S112
含む
含まない
トランザクションIDの生成
S113
Ks1を発生し、KPmc1にてKs1を暗号化{Ks1}Kmc1の生成
S114
トランザクションID//{Ks1}Kmc1の出力
S116
トランザクションID//{Ks2//KPm1//CRL_dat}Ks1を受信し、Ks1にて復号Ks2、KPm1及びCRL_datの受理
S126
S128
コンテンツID、ACに従って、ライセンスID、AC1、AC2の生成
S130
Kcをデータベースより取得
S132
Kc、AC2、ライセンスID、コンテンツIDとAC1をKPm1にて暗号化{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1の生成
S133へ
S170へ
トランザクションID//{Ks1}Kmc1の受理
S118
{Ks1}Kmc1を受けて、Kmc1にて復号Ks1の受理
S120
Ks2を発生し、Ks2、KPm1、CLR_datをKs1にて暗号化{Ks2//KPm1//CRL_dat}Ks1の出力
S122
トランザクションID//{Ks2//KPm1//CRL_dat}Ks1の送信
S124

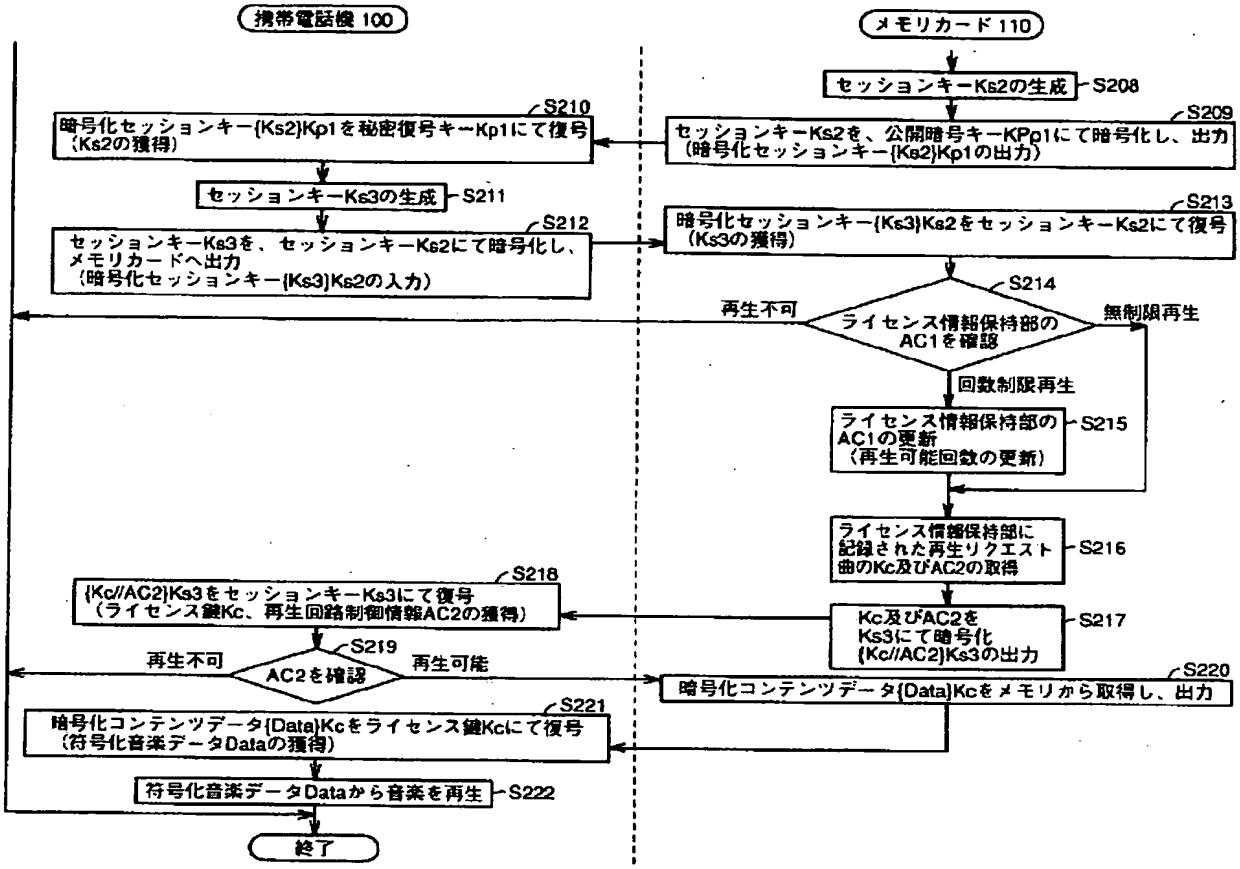
【図１０】


配信サーバ30
携帯電話機100
メモリカード110
配信(一部のみ)
S110,S112より
S132より
S133
CRL_datが最新？
Yes
No
S137
CRL_datをCRLデータベースより取得
S136
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datを
Ks2にて暗号化
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の出力
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の受信
S140
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1を
Ks2にて暗号化し、
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1}Ks2の送信
S134
{{Kc//AC2//ライセンスID//コンテンツID//
AC1}Km1}Ks2の受信
S135
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の受理
S142
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datをKs2にて復号
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datの受理
メモリ内のCRLを受理したCRL_datに書き換え
S144
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1}Ks2をKs2にて復号し、{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1を受理
S136
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1をKm1にて復号し、ライセンスID、コンテンツID、AC1,AC2,Kcの受理
S148
ライセンスID、コンテンツID、AC1、AC2,Kcをライセンス情報保持部に記録
S150
S152へ
S170へ

【図１１】


メモリカード 110
携帯電話機 100
配信サーバ 30
S150より
S152
データ取得
No
Yes
S154
トランザクションIDとコンテンツ配信要求の送信
S156
トランザクションID//コンテンツ配信要求の受信
S158
{Data}KcとData-infをコンテンツデータベースより取得し、
{Data}Kc//Data-infを送信
S160
{Data}Kc//Data-Infの受信
{Data}KcとData-infの受理
S162
{Data}KcとData-infをデータ領域に記録
S164
トランザクションID//配信受理を送信
S166
トランザクションID//配信受理を受信
S168
終了処理
(配信記録を配信記録データベースに記録)
S170
終了
終了

【図１４】



フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｇ１０Ｋ　15/02		Ｇ１０Ｋ　15/02		
Ｇ１０Ｌ　19/00		Ｈ０４Ｍ　1/00	Ｒ	
Ｈ０４Ｍ　1/00			11/00	３０２
11/00	３０２	Ｇ０６Ｆ　13/00		５１０Ｇ
// Ｇ０６Ｆ　13/00	５１０	Ｇ１０Ｌ　9/00		Ｎ